FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

PRESS RELEASE
2. January 2012

Turning smartphones into secure and versatile keys

It's already possible to open doors using an app – but we are a long way from seeing widespread acceptance of this in the market. Now, researchers have developed a piece of software that will make the technology even more secure and versatile.

Smartphones and tablets have become an integral part of our daily lives. The capabilities of these handily sized mini-computers seem almost boundless as we phone friends, shoot holiday snaps, lose ourselves in a new music download or access the internet to obtain the boarding card for our next flight in comfort. Does it not seem logical, then, that we should make use of these constant companions as the key to our cars, front doors or lockers as well? A few such solutions are already available, but what's still missing is widespread market acceptance. At this year's CeBIT trade fair in Hannover (March 5-9, 2013), researchers from the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt will be demonstrating their Key2Share software, a solution which will make the key app concept even more versatile and secure.

"In essence, Key2Share offers two new functions: users can issue digital keys remotely and assign these keys certain user permissions. For instance, I can grant the building superintendent access to my apartment for a short period so that he can open the door for the gas meter to be read while I'm at work," explains Alexandra Dmitrienko from the SIT. "The solution is built around modern security technologies and can be easily integrated into existing access control systems." Key2Share sends electronic keys directly to the user's mobile phone, in the form of a QR code attached to an e-mail or MMS.

Protecting parcel stations from phishing

One thing that Dmitrienko and her team will also be demonstrating at CeBIT (Hall 9, Booth E08) is a parcel station where access rights to individual compartments are issued using Key2Share. "Recently, users of parcel stations have fallen victim to phishing attacks. Equally, hackers continue to target their efforts on smartphones. In light of this, the big challenge was to protect the electronic keys without compromising the intuitive operation of such devices," explains Dmitrienko.

Key2Share works using the Near Field Communication (NFC) transmission standard, which allows data to be exchanged wirelessly over short ranges of up to a few centimeters."To open a door, all you need to do is hold your mobile phone close to the lock," says Dmitrienko. NFC interface and door locks only operate within a narrow bandwidth and have limited computing power. Consequently, scientists at the SIT have equipped Key2Share with particularly resource-efficient communication protocols. Further, electronic keys are reliably protected on the smartphone from malware and unauthorized access. This is achieved by leveraging advanced technologies which keep sensitive data on the smartphone separate from other data and apps (e.g. Fraunhofer's BizzTrust).

Communication between the mobile phone and a central server is protected by established security protocols. "And even if this communication is hacked into, it's impossible for unauthorized people to gain access to the digital key. This is because opening the door requires information contained both in the encrypted token sent to the user and in the app installed on their smartphone," clarifies Dmitrienko. Alongside front doors and parcel or locker compartments, the research scientist also suggests that the technology could potentially be applied to help administer keys in hotels or as part of car-sharing schemes. "The trend towards a 'shareconomy' will benefit the further development of this technology," concludes Dmitrienko. So the era of mobile phones as keys is one step closer.

Caption

Secure and flexible key management with smartphones
© Fraunhofer SIT

In regard to the use of pictorial material: use of such material in this press release is remuneration-free, provided the source is named. The material may be used only in connection with the contents of this press release.